DEPARTMENT OF GENERAL SERVICES

REPORT ON AUDIT
FOR THE PERIOD
JULY 1, 2012 THROUGH JUNE 30, 2015

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

Our audit of the Department of General Services (General Services) for the period July 1, 2012, through June 30, 2015, found:

- proper recording and reporting of all transactions, in all material respects, in the PeopleSoft Financials and the Commonwealth Accounting and Reporting Systems;

- certain matters involving internal control and its operation necessary to bring to management's attention; and

- certain instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

–TABLE OF CONTENTS–

AUDIT FINDINGS AND RECOMMENDATIONS

Improve Information Security Program

General Services is not properly managing certain aspects of its Information Security Program as required by the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard), and recommended by industry best practices.

We identified and communicated six weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

General Services does not have an adequate risk management process to consistently assess and protect its sensitive systems. Additionally, General Services does not document and implement information technology (IT) systems hardening policies, procedures, and practices effectively to ensure that IT systems are protected from potential continuity and data hardening risks and vulnerabilities. The identified internal control weaknesses increase the risk that General Services will not maintain compliance with the Security Standard, and industry best practices. General Services attributes the lack of controls to high turnover in key staff positions, including the agency head, CIO, and ISO. General Services should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard.

Improve Application Controls – Repeat Finding

As noted in the past three audits going back to fiscal year 2007, General Services does not adequately monitor application access for its critical financial application, PeopleSoft. We reviewed PeopleSoft access controls to ensure adequate segregation of duties, timely termination of user access, and that user privileges are reasonable based on responsibilities. Our review found the following deficiencies:

- Two employees continue to maintain "ALLPAGES" access within PeopleSoft.
- Three employees, including both employees with "ALLPAGES" access, have access to both enter and approve vouchers within PeopleSoft.
- Four employees have access to update receivable balances and enter and approve entries to the general ledger.
- PeopleSoft administrators are not performing and maintaining adequate documentation of periodic reviews of user access.
- General Services does not have formal policies and procedures for granting and terminating PeopleSoft access.
- General Services does not document and maintain a conflict matrix for PeopleSoft roles.

The Security Standard, AC-1 Access Control Policy and Procedures, requires agencies to develop, disseminate, and annually review/update, formal documented procedures to facilitate the

implementation of the access control policy and associated access controls. Additionally, the Security Standard Section 8.1 AC-2(c) and (d) requires that agencies establish conditions for group membership and specify access privileges. Finally, the Security Standard, AC-5, states that organizations should separate duties of individuals as necessary, and define information system access authorizations to support separation of duties.

The lack of policies and procedures, including annual access reviews and ensuring adequate segregation of duties, significantly increases the risk of unauthorized transactions in PeopleSoft. In particular, the "ALLPAGES" access in PeopleSoft is extremely high risk, as it allows individuals total control of all functions within the PeopleSoft system. As a result, management is increasing its risk of granting employees access they do not need, including violating the concept of separation of duties and creating internal control weaknesses.

The issues identified above are due to a lack of management oversight regarding the access granted and maintained in PeopleSoft. General Services should develop policies and procedures governing system access control and remove the high-risk user access noted above. In addition, General Services should also perform periodic reviews and maintain documentation of these reviews to ensure access is in agreement with the user responsibilities. Continuous monitoring of access to information systems, which are critical to the agencies' financial operations, also helps to mitigate the risk of errors and fraud.

Improve Oversight of Third-Party Service Providers

General Services did not obtain assurance over the outsourced functions provided by the Ariba Supplier Network (ASN) or Global Infrastructure Services (GIS). GIS provides managed computer hosting services for the CGI eProcurement Solution, including operations monitoring, infrastructure administration, environmental controls, and restricting physical access to the data center, which hosts Commonwealth data. The Service Organization Control (SOC) 1 Type II audit of CGI does not extend to the ASN or to the physical and environmental security controls of GIS. Additionally, General Services did not document a review of the SOC 1 Type II audit report of CGI.

Section 1.1 of the Security Standard states that agency heads remain accountable for maintaining compliance with the Security Standard in instances where IT equipment, systems, and services are outsourced to third-party service providers, and must enforce compliance with the Security Standard through documented agreements and oversight of the services provided. In addition, as of September 2015, Topic 10305 of the Commonwealth Accounting Policies and Procedures (CAPP) Manual requires agencies to have adequate interaction with their third-party service providers in order to gain an understanding of the service provider's control environment.

By not enforcing compliance with the Security Standard and not having a process to gain assurance over outsourced services, General Services cannot determine that the service provider's internal control environment is operating effectively and adequately protecting Commonwealth data and processes. General Service's management was not aware of the requirement to obtain assurance over subservice providers excluded from the CGI SOC report. Additionally, while the audit

report of CGI is discussed by General Services at the eVA Executive Steering Committee meetings, management did not consider documenting this discussion and the results of those discussions.

General Services should implement procedures for gaining appropriate assurance over all operations of service providers that impacts the Commonwealth's IT environment and sensitive data. Further, General Services should develop and implement policies and procedures for reviewing and documenting evaluations of SOC reports or other forms of assurance reports to ensure that the third-parties' security controls comply with the requirements described in the Security Standard. To maintain consistency and continuity, General Services should develop and implement procedures for documenting final decisions and action items that come as a result of the SOC report evaluation process. Finally, General Services should maintain oversight over this process to confirm compliance with the requirements in the CAPP Manual and Security Standard.

Improve PeopleSoft to CARS Reconciliation Process

General Services is not adequately performing reconciliations between its internal financial system, PeopleSoft, and the Commonwealth Accounting and Reporting System (CARS). The reconciliations reviewed did not indicate who performed or approved the reconciliations, or when the reconciliations were completed. In addition, beginning in January 2016, the individual performing the reconciliations has also been responsible for approving over half of the required reconciliations. Lastly, the reconciliations did not follow a clear methodology, and General Services does not have policies and procedures to support the reconciliation process.

CAPP Manual Topic 20905 requires all internally prepared accounting records to be reconciled to CARS to ensure accuracy and uniformity within CARS. The CAPP Manual states that agency reconciliations should create an audit trail so that the reconciliation can be traced to both source documents and CARS reports. The manual also expressly requires that agencies have detailed internal written procedures for meeting all CARS reconciliation requirements.

As stated in the CAPP Manual, lack of complete and up-to-date internal policies and procedures reflects inadequate internal control. Without proper policies and procedures, General Services cannot ensure the necessary level of quality control; therefore, accounting cannot produce useful reports. General Services should develop and maintain internal policies and procedures for performing reconciliations between PeopleSoft and CARS/Cardinal, and ensure that the policies and procedures, including proper segregation of duties, are implemented and followed. Although the Commonwealth is in the process of transitioning from CARS to Cardinal, CARS will remain the system of record for the Commonwealth through the end of fiscal year 2016, making it essential that reconciliations are performed properly during this time of transition.

Document *my*VRS Navigator Reconciliations and Policies and Procedures

General Services' Human Resources Division is not adequately documenting reconciliations between its internal human resources records and the Virginia Retirement System (VRS) *my*VRS Navigator system, which contains essential retirement data for state employees. Additionally,

management has not created *my*VRS Navigator policies or procedures to ensure reconciliations, changes, and adjustments in *my*VRS Navigator are performed accurately and by the appropriate employee.

The Department of Accounts Payroll Bulletin 2014-05 states that agencies should reconcile the creditable compensation amount in the Personnel Management Information System to the creditable compensation amount in *my*VRS Navigator each month before confirming the snapshot. In addition, the CAPP Manual Section 50410 and the VRS Employer Manual over Contribution Confirmation and Payment Scheduling also requires each agency to perform monthly reconciliations. Policies and procedures are necessary to detail how the requirements above are to be carried out and ensure segregation of duties exist when entering, reviewing, and approving the various adjustments within *my*VRS Navigator.

Without sufficient reconciliation documentation, there is no evidence indicating that General Services reviewed and processed all rejected transactions or potential discrepancies. Due to changes in the accounting and reporting standards over pensions, accurate management of compensation and contribution data at the employee level is critical to the Commonwealth's financial statements. In addition, General Services currently allows the individual who is entering adjustments to also approve adjustments, creating a segregation of duties issue.

General Services' Human Resources Division should develop *my*VRS Navigator policies and procedures to ensure compliance with *my*VRS Navigator reconciliation requirements, and ensure proper segregation of duties. The Human Resources Division should ensure its internal human resources data and *my*VRS Navigator properly reconcile, and retain sufficient documentation to demonstrate the identification and correction of reconciling discrepancies.

Improve Controls over Small Purchase Charge Card Reconciliations

General Services did not properly review and approve Small Purchase Charge Card (SPCC) users' monthly logs of transactions and associated documentation. Of the 21 logs sheets that were reviewed, four were not reviewed or signed by their supervisors. The supporting documentation for two of the log sheets could not be reconciled to the associated bank statement.

CAPP Manual Topic 20355 requires that cardholder's reconcile the statement to the purchasing log and supporting documentation to verify that purchases and returns are accurately listed on the statement. The CAPP Manual further requires an employee's supervisor to review and approve, by signing and dating, the reconciled SPCC statement before forwarding it to the accounting department within a time frame agreed upon by the purchasing and accounting units. In addition, the reconciliation of the SPCC purchase log, monthly statement, and supporting documentation must be made prior to the receipt of the following month's statement.

Not properly preparing and/or approving SPCC reconciliation logs may result in fraudulent transactions or purchases not being detected which may cause financial loss to General Services and the Commonwealth, inadequate documentation maintained to support and validate SPCC

transactions, or vendor overcharges that are not detected or corrected timely. Untimely approval and review of SPCC reconciliation packages resulted from insufficient oversight from supervisors and/or untimely submission of the reconciliation package by the cardholders. Improperly preparing the reconciliation was the result of employees' lack of awareness regarding their responsibilities, and insufficient oversight or guidance from supervisors.

General Services should ensure that SPCC reconciliations are prepared and reviewed in accordance with CAPP Manual Topic 20355 and educate and train cardholders to ensure requirements are followed. Since identifying these issues, General Services has revoked one of the charge cards in question and is requiring the employee to undergo SPCC reconciliation training

AGENCY HIGHLIGHTS

General Services provides support to other agencies by delivering a variety of services including, laboratory, engineering and architecture, procurement, real estate, vehicle management, and graphic design services. General Services serves not only Commonwealth agencies, but also local and federal government entities, as well as businesses and citizens.

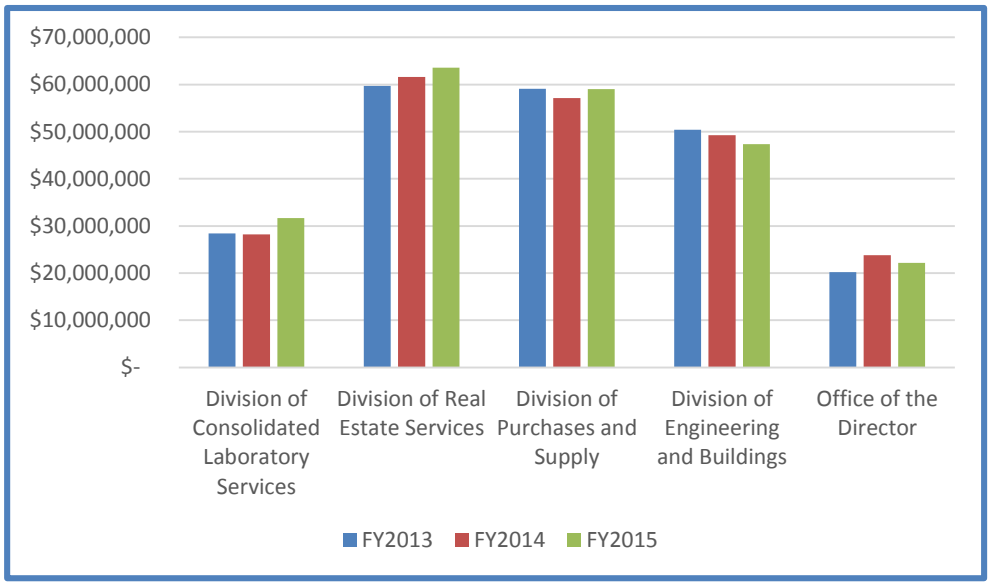
The Code of Virginia permits General Services' Director to organize the divisions of the agency to best meet the needs of the Commonwealth and to promote effectiveness and efficiency. Currently, the agency is organized as follows:

Office of the Director
Division of Real Estate Services
Division of Purchases and Supply
Division of Engineering and Buildings
Division of Consolidated Laboratory Services

General Services' largest divisions with respect to expenses are the Division of Real Estate Services, the Division of Purchases and Supply, and the Division of Engineering and Buildings as illustrated in Chart 1. The Office of the Director includes a variety of business units including Fiscal, Human Resources, Information Systems and Services, Office of Graphic Communication, Office of Surplus Property Management, and the Office of Fleet Management Services. Expenses for all five divisions have remained consistent over the past three fiscal years.

General Services Expenses by Program
Fiscal Years ended June 30, 2013, 2014, and 2015

Chart 1

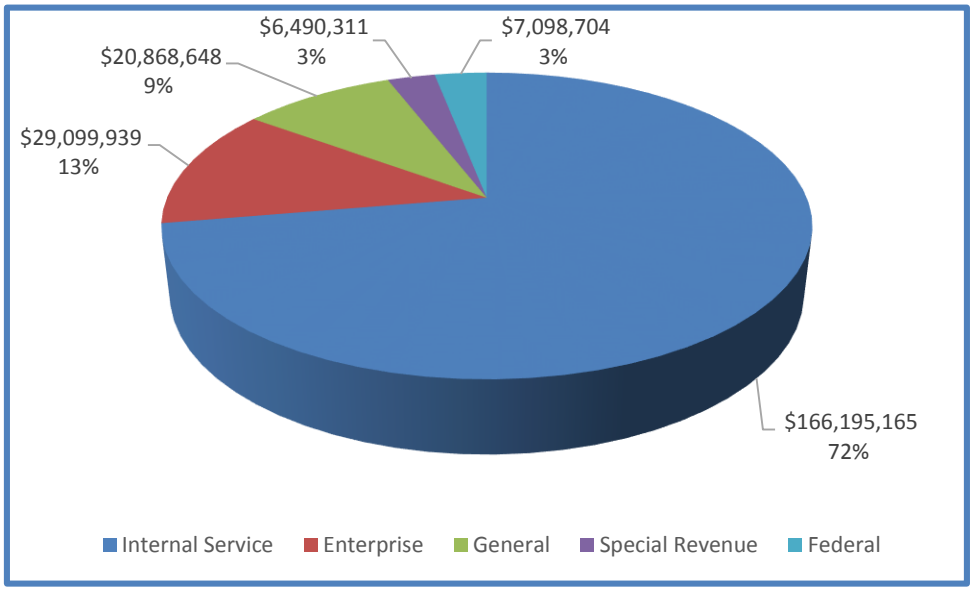


Source: Commonwealth Accounting and Reporting System
Note: Chart 1 depicts operating expenses and does not take into account capital outlay expenses.

Of the total funds appropriated to General Services, the majority of the funds are internal service and enterprise, 72 percent and 13 percent respectfully. The internal service funds are primarily comprised of rental of state buildings and sales from the central warehouse. Enterprise funds are generated by the Division of Purchases and Supply and the Division of Consolidated Laboratory Services. Agency and vendor eVA transactions fees totaled $18.2 million for fiscal year 2015. Special revenue mostly consists of parking fees which totaled $5 million in fiscal year 2015. As seen in Chart 2 below, approximately 88 percent of General Services' appropriations are generated by the agency.

Funding by Source

Chart 2



Source: Commonwealth Accounting and Reporting System
Note: Chart 2 does not include capital outlay.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

April 18, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Vice-Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Department of General Services** (General Services) for the period July 1, 2012, through June 30, 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objectives were to evaluate the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System and the PeopleSoft Financial System, review the adequacy of General Services' internal controls, test compliance with applicable laws, regulations, contracts, and grant agreements, and review corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

General Services' management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

Contractual services expenses
Contractual services procurement and management
Payroll
Small purchase charge card
*my*VRS Navigator
Financial reconciliations
System access controls
Information system security

We performed audit tests to determine whether General Services' controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, and contracts. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of General Services' operations. We tested transactions and performed analytical procedures, including budgetary and trend analyses.

Conclusions

We found that the Department of General Services properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System and PeopleSoft Financial System. The Department of General Services records its financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System.

We noted certain matters involving internal control and its operation and compliance with applicable laws and regulations that require management's attention and corrective action. These matters are described in the section entitled "Audit Findings and Recommendations."

The agency has not taken adequate corrective action with respect to the audit finding reported in the prior audit report. Therefore, we have repeated this finding in the section entitled "Audit Findings and Recommendations."

Exit Conference and Report Distribution

We discussed this report with management on May 17, 2016. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

JMR/clj

COMMONWEALTH *of* VIRGINIA

Department of General Services

Christopher L. Beschler
Director

Joseph F. Damico
Deputy Director

1100 Bank Street
Suite 420
Richmond, Virginia 23219
Voice (804) 786-3311
FAX (804) 371-8305

May 23, 2016

TO: Martha Mavredes, Auditor of Public Accounts

FROM: Christopher Beschler, Director, Department of General Services

SUBJECT: **RESPONSE TO FY13 - 15 AUDIT**

The following is the Department's response to the audit points contained in our FY 13 – 15 audit:

Point #1
Improve Information Security Program

General Services is not properly managing certain aspects of its Information Security Program as required by the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard), and recommended by industry best practices.

We identified and communicated six weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

General Services does not have an adequate risk management process to consistently assess and protect its sensitive systems, and does not document and implement Information Technology (IT) systems hardening policies, procedures, and practices effectively to ensure that IT systems are protected from potential continuity and data hardening risks and vulnerabilities. The identified internal control weaknesses increase the risk that General Services will not meet IT systems and data security standards for confidentiality, integrity, or availability. General Services attributes the lack of controls to high turnover in key staff positions, including the agency head, CIO, and ISO. General Services should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard.

DGS Response:
DGS management agrees with the finding and will address the issues identified. The addition of a full-time ISO will enable DGS to develop processes and procedures to minimize risks in these areas.

Point#2

Improve Application Controls – Repeat Finding

As noted in the past three audits going back to fiscal year 2007, General Services does not adequately monitor application access for its critical financial application, PeopleSoft. We reviewed PeopleSoft access controls to ensure adequate segregation of duties, timely termination of user access, and that user privileges are reasonable based on responsibilities. Our review found the following deficiencies:

- Two employees continue to maintain "ALLPAGES" access within PeopleSoft.
- Three employees, including both employees with "ALLPAGES" access, have access to both enter and approve vouchers within PeopleSoft.
- Four employees have access to update receivable balances and enter and approve entries to the general ledger.
- PeopleSoft administrators are not performing and maintaining adequate documentation of periodic reviews of user access.
- General Services does not have formal policies and procedures for granting and terminating PeopleSoft Access.
- General Services does not document and maintain a conflict matrix for PeopleSoft roles.

The Commonwealth Information Security Standard, SEC 501-09 AC-1 Access Control Policy and Procedures requires agencies to develop, disseminate, and annually review/update, formal documented procedures to facilitate the implementation of the access control policy and associated access controls. Additionally, SEC 501-09: Section 8.1 AC-2(c) and (d) requires that agencies establish conditions for group membership and specify access privileges. Finally, SEC 501-9 AC-5 states that organizations should separate duties of individuals as necessary, and define information system access authorizations to support separation of duties.

The lack of policies and procedures, including annual access reviews and ensuring adequate segregation of duties, significantly increases the risk of unauthorized transactions in PeopleSoft. In particular, the "ALLPAGES" access in PeopleSoft is extremely high risk, as it allows individuals total control of all functions within the PeopleSoft system. As a result, management is increasing its risk of granting employees access they do not need, including violating the concept of separation of duties and creating internal control weaknesses.

The issues identified above are due to a lack of management oversight regarding the access granted and maintained in PeopleSoft. General Services should develop policies and procedures governing system access control and remove the high-risk user access noted above. In addition, General Services should also perform periodic reviews and maintain documentation of these reviews to ensure access is in agreement with the user responsibilities. Continuous monitoring of access to information systems, which are critical to the agencies' financial operations, also helps to mitigate the risk of errors and fraud.

DGS Response:
DGS management agrees with the finding. Staffing has been augmented that will allow for more appropriate segregation of duties. The DGS Controller and Information Systems Services Director have been tasked with reviewing and documenting the necessary procedures to comply with the recommendations.

Point#3
Improve Oversight of Third-Party Service Providers

General Services did not obtain assurance over the outsourced functions provided by the Ariba Supplier Network (ASN) or Global Infrastructure Services (GIS). GIS provides managed computer hosting services for the CGI eProcurement Solution, including operations monitoring, infrastructure administration, environmental controls, and restricting physical access to the data center, which hosts Commonwealth data. The Service Organization Control (SOC) 1 Type II audit of CGI does not extend to the ASN or to the physical and environmental security controls of GIS. Additionally, General Services did not document a review of the SOC 1 Type II audit report of CGI.

Section 1.1 of the Commonwealth's Information Security Standard, SEC501-09 (Security Standard) states that Agency Heads remain accountable for maintaining compliance with the Security Standard in instances where IT equipment, systems, and services are outsourced to third-party service providers, and must enforce compliance with the Security Standard through documented agreements and oversight of the services provided. In addition, as of September 2015, topic 10305 of the Commonwealth Accounting Policies and Procedures (CAPP) Manual requires agencies to have adequate interaction with their third-party service providers in order to gain an understanding of the service provider's control environment.

By not enforcing compliance with the Security standard and not having a process to gain assurance over outsourced services, General Services cannot determine that the service provider's internal control environment is operating effectively and adequately protecting Commonwealth data and processes. General Service's Management was not aware of the requirement to obtain assurance over subservice providers excluded from the CGI SOC report. Additionally, while the audit report of CGI is discussed by General Services at the eVA Executive Steering Committee meetings, management did not consider documenting this discussion and the results of those discussions.

General Services should implement procedures for gaining appropriate assurance over all operations of service providers that impacts the Commonwealth's IT environment and sensitive data. Further, General Services should develop and implement policies and procedures for reviewing and documenting evaluations of SOC reports or other forms of assurance reports to ensure that the third-parties' security controls comply with the requirements described in the Security Standard. To maintain consistency and continuity, General Services should develop and implement procedures for documenting final decisions and action items that come as a result of the SOC report evaluation process. Finally, General Services should maintain oversight over this process to confirm compliance with the requirements in the CAPP Manual and Security Standard.

DGS Response:
DGS management agrees with the finding. The DGS Division of Purchases and Supply (DPS) is implementing procedures to assure compliance with the Commonwealth's Information Security Standard, SEC501-09. DPS will also ensure that the procedures will incorporate compliance with CAPP Manual, CAPP Topic 10305, which went into effect September 2015 after the review period of this report. Additionally, we now maintain documentation of our weekly review with our service provider on security controls.

Point#4
Improve PeopleSoft to CARS Reconciliation Process

General Services is not adequately performing reconciliations between its internal financial system, PeopleSoft, and the Commonwealth Accounting and Reporting System (CARS). The reconciliations reviewed did not indicate who performed or approved the reconciliations, or when the reconciliations were completed. In addition, beginning in January 2016, the individual performing the reconciliations has also been responsible for approving over half of the required reconciliations. Lastly, the reconciliations did not follow a clear methodology, and General Services does not have policies and procedures to support the reconciliation process.

CAPP Manual, Topic 20905 requires all internally prepared accounting records to be reconciled to CARS to ensure accuracy and uniformity within CARS. The CAPP Manual states that agency reconciliations should create an audit trail so that the reconciliation can be traced to both source documents and CARS reports. The manual also expressly requires that agencies have detailed internal written procedures for meeting all CARS reconciliation requirements.

As stated in the CAPP manual, lack of complete and up-to-date internal policies and procedures reflects inadequate internal control. Without proper policies and procedures, General Services cannot ensure the necessary level of quality control, therefore accounting cannot produce useful reports. General Services should develop and maintain internal policies and procedures for performing reconciliations between PeopleSoft and CARS/Cardinal, and ensure that the policies and procedures, including proper segregation of duties, are implemented and followed. Although the Commonwealth is in the process of transitioning from CARS to Cardinal, CARS will remain the system of record for the Commonwealth through the end of fiscal year 2016, making it essential that reconciliations are performed properly during this time of transition. `

DGS Response:
DGS management agrees with this point and the recommendations. The DGS Controller will be responsible for implementing the necessary changes to comply with the recommendations.

Point#5
Document VNAV Reconciliations and VNAV Policies and Procedures

General Services' Human Resources Division is not adequately documenting reconciliations between its internal human resources records and the Virginia Retirement System

(VRS) myVRS Navigator (VNAV) system, which contains essential retirement data for state employees. Additionally, management has not created VNAV policies or procedures to ensure reconciliations, changes, and adjustments in VNAV are performed accurately and by the appropriate employee.

The Department of Accounts Payroll Bulletin 2014_05 states that agencies should reconcile the creditable compensation amount in PMIS to the creditable compensation amount in VNAV each month before confirming the snapshot. In addition, the CAPP Manual Section 50410 and the VRS Employer Manual over Contribution Confirmation and Payment Scheduling also requires each agency to perform monthly reconciliations. Policies and procedures are necessary to detail how the requirements above are to be carried out and ensure segregation of duties exist when entering, reviewing, and approving the various adjustments within VNAV.

Without sufficient reconciliation documentation, there is no evidence indicating that General Services reviewed and processed all rejected transactions or potential discrepancies. Due to changes in the accounting and reporting standards over pensions, accurate management of compensation and contribution data at the employee level is critical to the Commonwealth's financial statements. In addition, General Services currently allows the individual who is entering adjustments to also approve adjustments, creating a segregation of duties issue.

General Services' Human Resources Division should develop VNAV policies and procedures to ensure compliance with VNAV reconciliation requirements, and ensure proper segregation of duties. The Human Resources Division should ensure its internal human resources data and VNAV properly reconcile, and retain sufficient documentation to demonstrate the identification and correction of reconciling discrepancies.

DGS Response:
DGS management agrees that it is essential that VRS retirement data for our employees match the DGS personnel records. The reconciliations reviewed were performed in accordance with the VRS Employer Manual, and to our knowledge, no discrepancies were identified.

DGS is committed to taking the recommended actions and will develop written procedures on formally reviewing and documenting rejected transactions and discrepancies and will develop written procedures for properly reconciling VNAV records with the Personnel Management Information System (PMIS) data. In addition, workflow procedures to ensure proper segregation of duties and retention of sufficient documentation will be implemented.

Point#6
Improve Controls over Small Purchase Charge Card Reconciliations

General Services did not properly review and approve Small Purchase Charge Card (SPCC) users' monthly logs of transactions and associated documentation. Of the 21 logs sheets that were reviewed, four were not reviewed or signed by their supervisors. The supporting documentation for two of the log sheets could not be reconciled to the associated bank statement.

CAPP Manual topic 20355 requires that cardholder's reconcile the statement to the purchasing log and supporting documentation to verify that purchases and returns are accurately listed on the statement. The CAPP Manual further requires an employee's supervisor to review and approve, by signing and dating, the reconciled SPCC statement before forwarding it to the accounting department within a time frame agreed upon by the purchasing and accounting units. In addition, the reconciliation of the SPCC purchase log, monthly statement, and supporting documentation must be made prior to the receipt of the following month's statement.

Not properly preparing and/or approving SPCC reconciliation logs may result in fraudulent transactions or purchases not being detected which may cause financial loss to General Services and the Commonwealth, inadequate documentation maintained to support and validate SPCC transactions, or vendor overcharges that are not detected or corrected timely. Untimely approval and review of SPCC reconciliation packages resulted from insufficient oversight from supervisors and/or untimely submission of the reconciliation package by the cardholders. Improperly preparing the reconciliation was the result of employees' lack of awareness regarding their responsibilities, and insufficient oversight or guidance from supervisors.

General Services should ensure that SPCC reconciliations are prepared and reviewed in accordance with CAPP 20355 and educate and train cardholders to ensure requirements are followed. Since identifying these issues, General Services has revoked one of the charge cards in question and is requiring the employee to undergo SPCC reconciliation training.

DGS Response:
DGS management agrees with this finding and recommendation. Management will ensure that cardholders and supervisors complete their annual SPCC training. In addition, management will ensure that reconciliation logs are reconciled and signed by the cardholder and the supervisor/reviewer before the log will be accepted by DGS' Central Procurement Unit (CPU) and DGS Fiscal Services. By signing the reconciliation log both the cardholder and supervisor/reviewer are verifying that the documentation is complete, all purchases are valid, for state use, and are compliant with all procurement regulations.

Each Contracting Officer in CPU will review at least one cardholder per month. The review will encompass several months of reconciliation files. If a violation is detected, corrective action will be taken and verified through a second review.

DEPARTMENT OF GENERAL SERVICES

(as of June 30, 2015)

Nancy Rodrigues
Secretary of Administration

Christopher L. Beschler
Director, Department of General Services

Joseph Damico
Deputy Director, Department of General Services

Bryan W. Wagner
Controller, Department of General Services